TOP SECRET

TICOM/I-37

TRANSLATION OF PAPER WRITTEN BY

REG. RAT. DR. HUETTENHAIN OF OKW/CHI

ON

SPECIAL APPARATUS USED AS AIDS TO CRYPTANALYSIS.

The attached paper was written at FLENSBURG in June 1945 by Dr. HUETTENHAIN, at the request of TICOM Interrogating Officers.

It elaborates the descriptions of the five special machines referred to in paragraph 12, etc., of TICOM/I-31, and also gives an account of further similar devices developed, or under construction, or planned.

TICOM
14 July, 1945

No. of pages:

DISTRIBUTION:

British
Director
D.D.3
D.D.4
D.D.(N.S.)
D.D.(M.W.)
D.D.(A.S.)
A.D.(C.C.R.)(2)
Lt. Col. Leathem

U.S.
OF 20-G (2)(via Lt. Pendergrass)
G-2 (via Lt. Col. Hilles)
S.S.A.(2)(via Major Seaman)
Director, S.I.D. ETOUSA (via Lt. Col. Johnson)

Ticom
Chairman
S.A.C. (2)
Cdr. Bacon
Cdr. MacKenzie
Cdr. Tandy
Lt. Col. Johnson
Lt. Cdr. Manson
Major Seaman
Lt. Eachus
Lt. Vance
Capt. Cowan
Lt. Fehl
Ticom Files (2)

Additional
Major Morgan (2)
A.D. (Mch)

I-37

APPARATUS USED AS AIDS TO CRYPTANALYSIS

Introduction: In order to save time and staff, machines are used for identifying codes and cyphers and for breaking identified codes and cyphers. Hollerith machines are always suitable for this purpose when it is a question of sorting processes. In order to be able, by means of machinery, to work on problems of cryptography which cannot be traced back to a sorting process, cryptanalytical apparatuses were developed, built and put into use.

First of all the completed cryptanalytical apparatus will be described, and then those that were planned or being completed. Technical details cannot be given as there are no data here and this author has little technical knowledge.

A) Completed apparatuses

1) Roller Apparatus

The Roller apparatus is used for forming differences between at the most 30 figure groups of up to 5 digits.

5 metal rods, 1-5, each carry 30 rollers, the circumferences of which are marked in sequence with the figures 0, 1, 2, 3, 4.....8, 9. On every rod there is in addition a roller right at the top, somewhat away from the others, and fixed to the rod.

Each of the 30 rollers can be set at one of the 10 possible positions. The 5 rods can be revolved on their longitudinal axes and take the rollers round with them.

If, for example, all differences mod. 10 are to be formed between 20 5-figure cypher groups on the same subtractor (SCHLUESSELGLEICH), then first of all the 5 rods are turned round until the figure 0 appears on all at the top (see fig. 1). Then the figures of the first 5-figure group are turned up to the top on the first roller of each of the five rods (in fig. 1, 13870). The figures of the second cypher group are then turned up to the top on the second roller of each of the five rods (44651) etc., until all 20 groups have been set.

If now each of the 5 rods is so turned that in the windows in which the first cypher group was set only noughts appear, then the other 5-figure groups represent the differences mod. 10 between the first group and the other 19. If the five rods are so turned that only noughts appear in the second group, then there will appear in the horizontal rows all differences mod. 10 between the second groups and the other 19 etc.

If there appears among these differences one which also appears in the previously prepared difference catalogue (i.e. a collection of all the differences between the most frequent code groups, then the 2 cypher groups, between which there is this difference, are transformed by turning the 5 rods into those groups out of which the difference in the difference catalogue was produced. There now stands in the top row of figures the reduction number for the 20 cypher groups taken in the example. The 20 cypher groups themselves are reduced to the base of the groups of the difference catalogue. It is therefore easy to check up whether the reduction is correct or not.

The apparatus has an openable lid so that only the figures at the top of each roller can be seen at any time. The apparatus also has a collapsable leg at the back, up by the knobs, so that it can be stood at a slant on the table.

The roller apparatus is also built for printing (in conjunction with the Naval Cryptanalysis Station). The figures on the rollers are made in relief, as mirrored images. If printing ink is smeared on and then a sheet of paper placed over them, the figure groups at every setting can be recorded. The setting of the figures on the printing apparatus is done from right to left.

2) Difference calculating Apparatus

The difference calculating apparatus calculates differences mod. 10 between numbers and writes down these numbers.

The apparatus consists of:

1) The reading, 2) the calculating, and 3) the recording apparatus. (see figure 2)

2 differences calculating apparatus have been built, one working with, one without, storage (SPEICHERUNG).

a) With storage

1) The reading apparatus (ABTASTGERAET).

The figure groups between which the differences are to be worked out, are punched on to a tape. A duplicate of this tape is made. Both these strips are placed in the reading apparatus. The reading apparatus is a little box in which photo cells are housed. The perforated strips are read photo-electrically. One perforated strip is stuck together so as to form an endless loop while the other can remain as a strip.

Both perforated strips are placed into reading apparatus in the initial position. When the starting knob is pressed, the strip moves to the extent of e.g. 1 5-figure group, while the endless loop, (SCHLEIFEN-STREIFEN) still remains stationary. When the strip (BANDSTREIFEN) comes to rest, the loop begins to move, and moves through one complete turn. Then the strip makes a 5-group move and the loop again makes a complete turn, and so on until all the five-figure groups of the strip have come up once. All movements are completely automatic, being guided by interpolation of certain 5-symbol signs on the perforated strip. Only the starting is done by hand.

2) The calculating apparatus (RECHENGERAET)

In the calculating apparatus, the first 5-symbol group of the strip will be translated into 5 figures and stored after the pressing of the starting knob. If the endless loop now moves, the 5-symbol signs in the calculating apparatus will likewise be transposed into figures and subtracted mod. 10, digit by digit, from the 5 figures of the strip which have been stored.

The processes of storage and subtraction are carried out by a number of electrical relays.

The result of this subtraction is then passed on out of the calculating apparatus into the:

3) Recording Apparatus (REGISTRIERGERAET)

This is an electrical typewriter, which is modified in such a way that the 10 figure keys are provided with electric magnets. When an impulse is received on one of these magnets, the magnet attracts the appropriate figure

The roller apparatus is also built for printing (in conjunction with the Naval Cryptanalysis Station). The figures on the rollers are made in relief, as mirrored images. If printing ink is smeared on and then a sheet of paper placed over them, the figure groups at every setting can be recorded. The setting of the figures on the printing apparatus is done from right to left.

2) Difference calculating Apparatus

The difference calculating apparatus calculates differences mod. 10 between numbers and writes down these numbers.

The apparatus consists of:

1) The reading, 2) the calculating, and 3) the recording apparatus. (see figure 2)

2 differences calculating apparatus have been built, one working with, one without, storage (SPEICHERUNG).

a) With storage

1) The reading apparatus (ABTASTGERAET).

The figure groups between which the differences are to be worked out, are punched on to a tape. A duplicate of this tape is made. Both these strips are placed in the reading apparatus. The reading apparatus is a little box in which photo cells are housed. The perforated strips are read photo-electrically. One perforated strip is stuck together so as to form an endless loop while the other can remain as a strip.

Both perforated strips are placed into reading apparatus in the initial position. When the starting knob is pressed, the strip moves to the extent of e.g. 1 5-figure group, while the endless loop, (SCHLEIFEN-STREIFEN) still remains stationary. When the strip (BANDSTREIFEN) comes to rest, the loop begins to move, and moves through one complete turn. Then the strip makes a 5-group move and the loop again makes a complete turn, and so on until all the five-figure groups of the strip have come up once. All movements are completely automatic, being guided by interpolation of certain 5-symbol signs on the perforated strip. Only the starting is done by hand.

2) The calculating apparatus (RECHENGERAET)

In the calculating apparatus, the first 5-symbol group of the strip will be translated into 5 figures and stored after the pressing of the starting knob. If the endless loop now moves, the 5-symbol signs in the calculating apparatus will likewise be transposed into figures and subtracted mod. 10, digit by digit, from the 5 figures of the strip which have been stored.

The processes of storage and subtraction are carried out by a number of electrical relays.

The result of this subtraction is then passed on out of the calculating apparatus into the:

3) Recording Apparatus (REGISTRIERGERAET)

This is an electrical typewriter, which is modified in such a way that the 10 figure keys are provided with electric magnets. When an impulse is received on one of these magnets, the magnet attracts the appropriate figure lever and the figure key of the typewriter strikes.

All three parts of this apparatus work in unison. When the carriage of the typewriter returns, the reading and the calculating apparatus both stop.

The speed of calculation is limited by the speed of striking of the typewriter to a maximum of 7 signs a second. Reading and calculating apparatus would permit of much higher speeds.

b) Without storage.

The difference calculating apparatus without storage works according to the same principle of calculation and registration; the reading in the reading apparatus is also done photo-electrically. Only the movement of the strip is different and, in consequence, the sequence of the recorded differences too.

In this case both strips are stuck so as to form loops. One loop is made one group longer than the other loop. After activation of the starting knob both loops begin to turn. While this is happening, the differences are worked out in the calculating apparatus, and they are then recorded in the registering apparatus. The following groups are thus subtracted from one another:

1 - 2, 2 - 3, 3 - 4, ... n - 1.

After one complete turn the one loop has moved one group relatively to the other. Now the differences of the following groups are formed:

1 - 3, 2 - 4, 3 - 5, ... n - 2.

This is continued until all the differences are worked out.

3) "WITZKISTE" ((See TICOM/I-31, page 2, para. 5. Dr. WITT - query WITZ.))

The purpose of the "WITZKISTE" is to reduce to a known base, without intermediate calculation, 4-symbol cypher groups recyphered on the same subtractor group. The following are prerequisites for working with the apparatus:

Knowledge of the most frequent book-groups and

A number of cypher groups on the same subtractor.

The cryptographic principle of the apparatus is as follows:

All the most common book groups are subtracted mod. 10 from each of the cypher groups on the same subtractor. On the assumption that some of the cypher groups have come from frequently-occurring book groups, then one difference - and that will then be the addition number - will occur especially frequently.

The technique of putting this principle into practice is as follows:

The most common book groups are made visible, in a quite definite order, on a black enamelled glass plate by removing the enamel (see fig. 3). The glass plate thus prepared is placed under a fixed lattice-frame (see fig. 4) according to each cypher group. In each setting the part of the glass plate which remains visible through the lattice-frame is photographed. The same film will then continue to be exposed as long as cypher groups of the same subtractor are to be reduced. The film is developed after exposure. The blackest point

is the reduction number sought. Since the lattice is photographed too the co-ordinates of the point can immediately be read off. This is best done by projecting the picture onto a screen by means of a lantern.

The 4-symbol book groups will be shown, according to co-ordinates, on a surface of 100 x 100. In consequence of the addition mod. 10 each of the most common book groups must appear 4 x 4 = 16 times. The lattice plate is so constructed that when placed on the code plate it shows once exactly each of the 10,000 possible points. The lines of the lattice are 9 units thick.

The code plate is placed by hand against the fixed lattice frame on to the cypher group in question.

The equal illumination of the whole of the lattice causes great difficulty.

The sum of the exposure times must be so chosen, that the "correct" point lies at the bend of the exposure-blackening-curve, while the other fortuitous blackenings do not yet assume prominence.

Experience must show how many code-groups are let into the code plate. Likewise, the size of the holes for each book-group must be determined by experience.

4) Sawyer's Jack (SAEGEBOCK)

The "Sawyer's Jack" phase-search apparatus. With its assistance it can be determined whether and where 2 different cypher texts are in phase. It can further be determined whether a period occurs in a single cypher text and how long the period is.

The cryptographic principle as the basis of the apparatus is as follows:

If 2 cypher texts are in phase (e.g. multiple or SPRINGCÄSAREN = periodic substitution) then the number of identical single elements, identical bigrams, trigrams etc. is a maximum.

The apparatus itself in this case too consists of reading, calculating and registering apparatus.

In the reading apparatus the 2 perforated strips are, in this case too, photo-electrically read at a speed of 75 (signs) a second.

Identical single elements, bigrams, trigrams up to parallels of the length of 10, are noted in the registering apparatus.

These findings are registered in the registering machine. It consists of 10 different writing devices. All writing devices work on a paper strip about 20 ins. wide. Each writing device makes a small dash when it receives from the calculating machine the order to do so. The little dashes of each writing device are combined to form a long dash in each case. When the message has been run through once, all the writing machines return automatically to nought and the process begins again from the beginning, after the paper strip has run on a little further.

Some of the writing devices can be cut out.

If, for example, only the counter which counts identical single elements is switched on and there is a column substitution of the period 7, then every 7th dash on the registering paper is especially long. (see figure 5).

5) "Tower Clock" [illegible]

The following cryptographic problem can be worked out on the "tower clock". One takes a number of cypher text passages on the same key (column periodic substitution) of known period (at the most 30) (the fact of being on the same key was discovered for example by cypher repeats). It has to be decided whether or not a passage of cypher text of the same length is on the same key as a depth already established (this problem occurs in the American strip system).

Say the cypher text passage to be examined is 30 elements long; and say there is a column substitution of the period 30. Let the 30 alphabets be marked 1-30.

The 30 cypher elements are punched on to a tape in the international 5 unit alphabet. This perforated strip is read in the reading apparatus of the "tower clock" photo-electrically, symbol by symbol. The speed of reading is about 1 symbol a second.

The cypher text passages already recognized as on the same key are stored in the calculating apparatus of the "tower clock" as a basis on which to start; and in such a way that for each of the substitution alphabets the elements receive different scores according to the frequency in the cypher texts. Provision is made for 5 different scores.

The first symbol on the tape receives in the calculating apparatus the score which the same symbol has received in alphabet 1. The pen of the recording apparatus makes on the paper strip a dash of the length of this score. This process is carried out with the remaining 29 symbols in the corresponding substitutions. A rotating distributor keeps cypher elements and substitutions in step. The pen totals the 30 scores in one more or less long dash. One can then tell from the length of the dash whether the cypher text passage being examined is on the same key as the base already collated or not.

The comparison of a passage of 30 elements is thus completed in half a minute. If in this way out of a large number of cypher text passages some are recognized as certainly belonging to the base, the base is increased to the extent of these passages, i.e. the scores in the calculating apparatus are improved.

Note
In correct addition to depth will make [illegible] more accurate

6) Bigram Apparatus

With the bigram apparatus 26 x 26 = 676 bigrams can be worked on. 2 perforated strips are read photo-electrically in the reading apparatus at a speed of 75 symbols a second.

With the aid of a cascade circuit (see figure 6), the 676 different bigrams are produced as single elements. For this nearly 700 relays are needed. These 676 different symbols end on the left part of the plug board in the calculating apparatus. This part of the plug board consists of 26 x 26 sockets. (see figure 7).

If the frequency of occurence of certain bigrams is known, then the bigrams can be divided according to their frequency in to 6 different classes. The right part of the plug board contains the values table. With the assistance of plug-leads every bigram of the element table can be given a value in the values table. The value nought is not plugged.

The registering machine records every single bigram, doing it by dashes of different lengths according to the value plugged. The paper of the registering machine is formed into a continuous loop and moves evenly along under the pen. The pen is fixed on a spindle, so that the recording on the paper band is done in spirals.

With the aid of this apparatus, transpositions, for instance, can be solved when the frequency of the bigrams is known.

With this apparatus it is also possible to find repeats (PARALLEL-STELLEN) and, in particular, broken repeats. For this purpose it is necessary to plug the principal diagonals aa, bb, --- zz on the element table, while all other bigrams remain unplugged.

7) Perforated Strip Calculating Apparatuses.

Perforated strip calculating devices are combinations of standard equipment such as perforated strip receivers and perforated strip transmitters.

The apparatus was used for testing the security of our own codes and cyphers, particularly of the cypher teleprinter machines and cypher attachments (SCHLUESSELZUSAETZE).

According to the circumstances of the problems the most varied use was made of this standard equipment, e.g.

A new perforated strip is produced from 2 perforated strips superimposed on one another, according to the law; identical conditions in the 2 original strips produce (hole), non-identical conditions produce - (no hole).

A new perforated strip is produced from a perforated strip in such a way that always when 2 identical conditions follow one another a hole results, when 2 non-identical conditions follow one another, no hole results - this happens for each of the 5 impulses separately.

The speed was 7 symbols a second.

8) Simple counting apparatus.

By means of the simple counting apparatus it is possible quickly to work out statistics, when there are not more than 100 different elements.

100 counting machines (Post Office counters) are put side by side. The text for which statistics are to be worked out is punched on to a tape. The perforated strip is read and the symbol in each case put on to the corresponding counter. The counters are read off and their position photographically recorded.

In practice this apparatus was used with success within the scope of the investigations into the security of our own systems.

B) Apparatus under construction and/or planned.

a) Apparatus for searching for repeats.

The apparatus for searching for repeats, planned and in part already in production, was not meant to solve the most exacting tasks of this kind. The task was rather to seek out as quickly as possible all repeats of the length 5 and more from a limited number of cypher texts (20-25 each of about 100 5-symbol groups: thus 10,000-12,500 elements).

The 10,000 letters were recorded one after the other as 5 unit alphabetical symbols on to an ordinary film. A duplicate was made.

Both strips were now to pass at high speed in front of a reader working without inertia. In the event of the 2 strips being completely identical for at least 5 letters, this passage would be likewise registered without inertia.

The strips were to pass before the reading device at a speed of 10,000 symbols a second. Accordingly, not quite 3 hours would have been required to work through 10,000 letters.

It was also only intended at first to record that repeats occurred thus, not yet how the passages read and exactly when they were.

This would have sufficed for the discovery of e.g. transposition compromises, which are founded on a code.

The apparatus would have been ready for experiments in about 3 months.

It was intended above all to test on this apparatus whether speeds of this magnitude could still produce accurate data.

b) Statistics recording apparatus

The statistics recording apparatus was to be a marked improvement on the simple counting apparatus.

It was to have been possible to record statistically 1,000 different elements: therefore 1,000 counters had to be built in.

Apart from single letters, it was to have been possible to examine also bigrams, split bigrams (a.b), (a..b), (a...b) etc., word beginnings, word ends, the second letter of words, the third letter of words, penultimate letter of words, vowels, etc. In short it was to have been possible quickly and surely to recognize all cryptographically interesting peculiarities of the various languages.

The speed of advance of the strip was estimated at 100 elements a second.

The apparatus would have been ready in about 4 months.

c) "WITZKISTE" with 5-symbol book-groups.

During the last weeks in Berlin it began to be deliberated whether the principle according to which the "WITZKISTE" handled the 4-symbol groups could be also employed on 5-symbol book groups.

Deliberations as to whether one of the 5 symbols could just be omitted led to no satisfactory solution. The possibility was then considered of dividing up the 5-symbol groups into 2 4-symbol groups. It had not been decided how the division was best to be made. If ABCDE is the five-letter group, the division ABCD and BCDE, or ABCD/ABCE, and others, were considered.

Final remarks.

Technical details of all apparatus are best known to Dipl. Ing. Rotscheidt and Jensen who developed them.

In general the aim was to build reading and recording apparatus in all conceivable forms, in order to be able to put together the suitable apparatus immediately a practical task turned up.

Translations of descriptions on Attached Diagrams.

Fig. 2. Endless band of tape.
Reading Apparatus.
Punched Tape.
Calculating Apparatus.
Recording Apparatus.

Fig. 3. Glass plate showing the recording of one code group.

Fig. 4. Lattice Plate.

Fig. 6. Cascade Connections.
This connection must be continued to the right, until 676 free exits occur.

Fig. 7. Plug-board.
Element Table.
Value Table.

(Trans.: KCK)

mit der
Darstellung
eines Punktes.

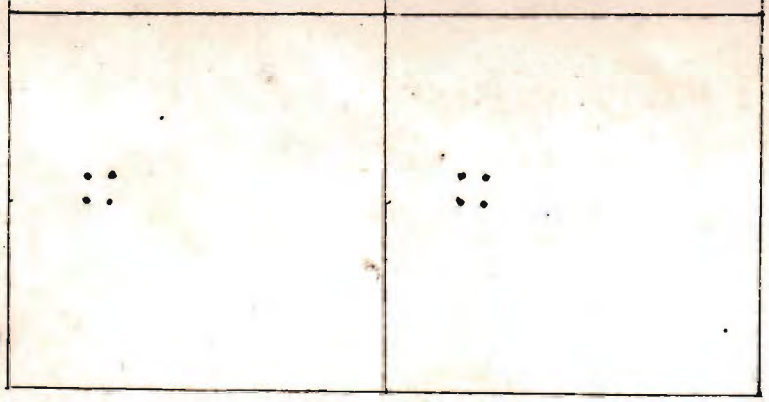
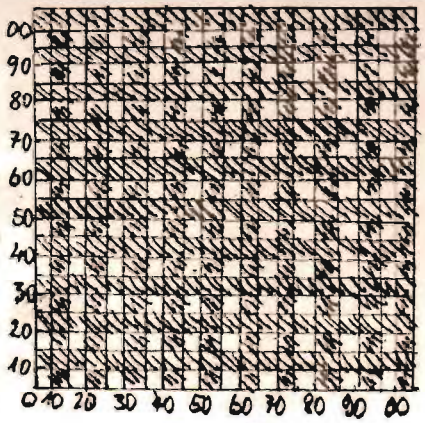
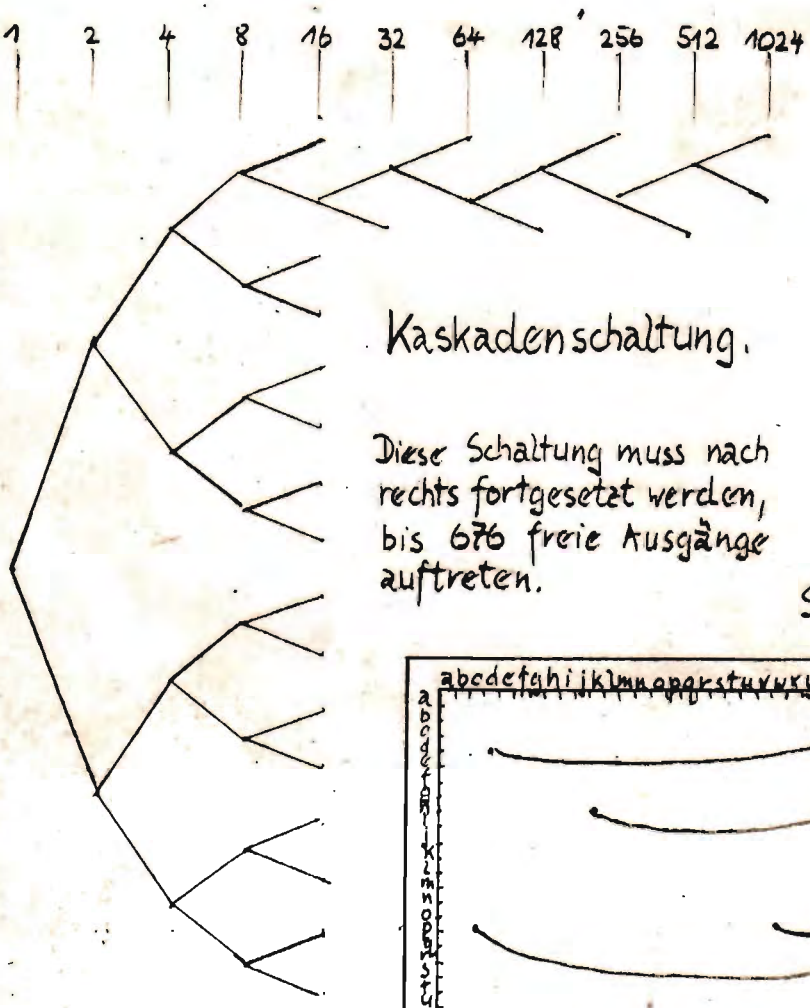


Fig. 3



Gitter-
platte

Fig. 4

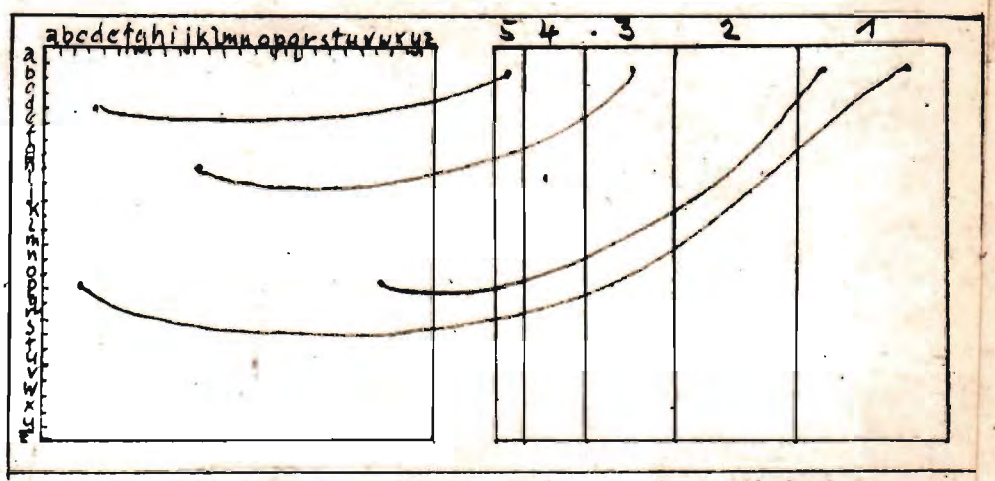


Kaskadenschaltung.

Diese Schaltung muss nach rechts fortgesetzt werden, bis 676 freie Ausgänge auftreten.

Fig. 6

Steckerbrett



Elementtafel

Wertigkeitstafel

Fig. 7

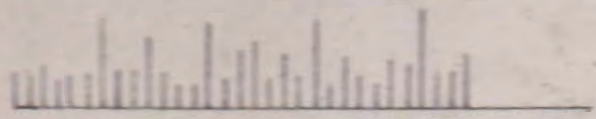


Fig. 5

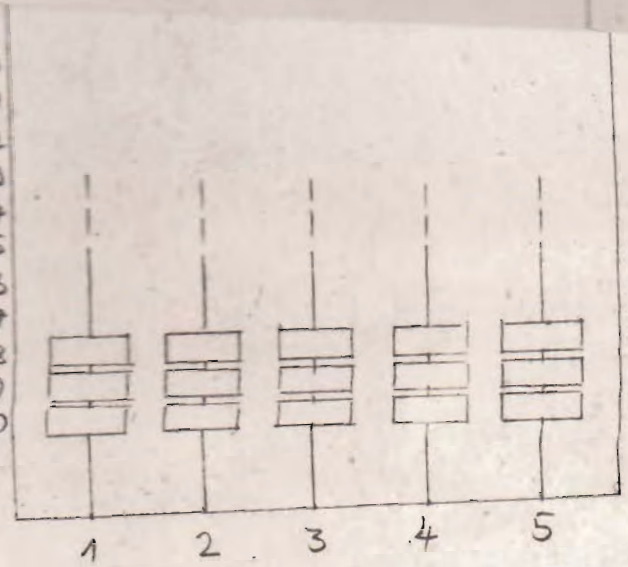


Fig. 1

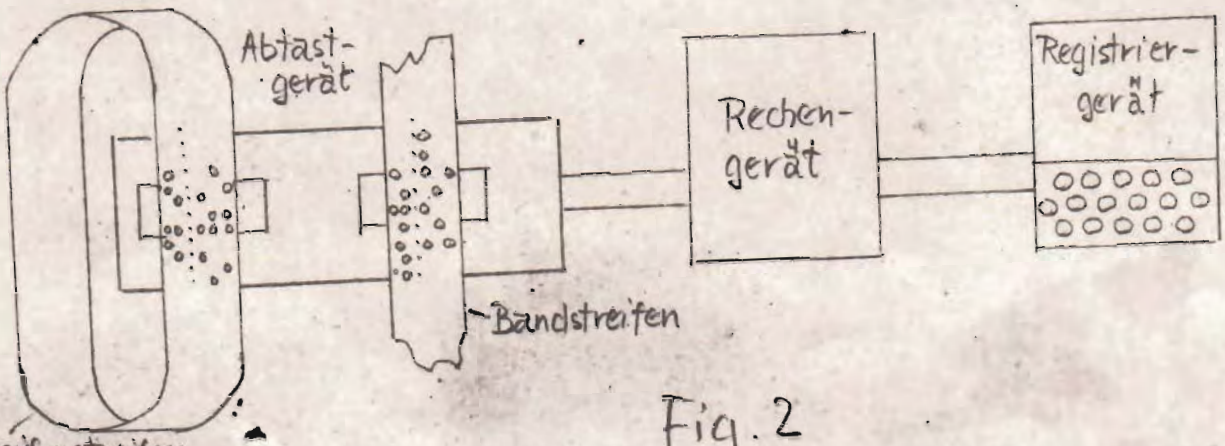


Fig. 2